S-172
Annex L
Item 3
Copy 2

~~TOP SECRET~~

TICOM/I-160

HOMEWORK BY SONDERFUEHRER KUEHN OF GEN. D. N.A.
ON GENERAL ORGANISATION AND WORK OF FRENCH REFERAT

Attached is a translation of homework done at the request of TICOM at U.S. Seventh Army Interrogation Centre in September 1945, by Sonderfuehrer (Z) Hans Wolfgang Kuehn, Head of the French Referat of In. 7/VI from 1941 to February 1945, giving the internal organisation, and a detailed report of French systems worked on in Kuehn's section.

Trans. H.D.

TICOM
3 November 1945

No. of Pages 22

DISTRIBUTION

British
D.D.I.
H.C.C.
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
C.C.R.
Commander Tandy
Major Morgan.

U.S.
OP-20-G (2) (via Lt.Cdr. Manson)
G-2 (via Lt.Col. Hilles)
A.S.A. (4) (via Major Seaman)
Director, S.I.D. USFET
Colonel Kunkel, USAAFE

TICOM
Chairman
S.A.C. (3)
Commander Bacon
Major Seaman
Lieut.Cdr. Manson
Major Cowan
TICOM Files (4)

ORGANISATION OF H.Q. OF GEN. DER N.A.

(= Director General of German Sigint)

Situation at Middle of March 45

Gen. d. N.A.
Oberst Boetzel

Section 1	Section 2	Section 3	Section 4	Section 5	Section 6	Section Z

Section 1:- Signals communications (Officer Responsible for Signals Routine)
(In this Section was Amtmann Bodenmueller)

Section 2:- Evaluation "West"
I/C Section: Hauptmann Thiele (or Thiel)
Oberinspektor Sernatinger
Oberinspektor Guske
Oberinspektor Buchfelder

Section 3:- Evaluation "East"
I/C Section: Hauptmann Gorzolla (or similar name)

Section 4:- Cryptanalysis
For detailed organisation see below

Section 5:- Captured material - obtaining books and data - maps
I/C Section: Amtmann Block

Section 6:- Unknown
At the date in question, the Section was in the neighbourhood of Stuttgart

Section Z:- Personnel matters

Organisation of Section 4
(Cryptanalysis)

I/C Section Major Dr. Hentze

Main Section 1 — Analytical work and work on machine ciphers

Head of Main Section:- Regierungsbaurat Dr. Pietsch

Sub-Section a - Analysis
Work on specially difficult systems
Head:- Regierungsbaurat Marquardt
Deputy:- Wachtmeister Hillburg

Sub-Section b - Machines
Work on all cipher machines
Head:- Wachtmeister Doering
Deputy:- Wachtmeister Buggisch (till about Nov.44)
later - Wachtmeister Valentin

Main Section 2 Cryptanalysis "West"

Head of Main Section:- Oberleutnant Kneschke
(previously Ober-Regierungsrat Bailovic - till Oct.44)
[Bailovic was transferred to H.Q. OKW/Chi]

Sub-Section a - U.S.A.
Great Britain
Sweden
Head:- Regierungsbaurat Dr. Werner Schulz
Deputy:- Wachtmeister Schanz (?)

(Previously U.S.A.) / Sweden) one Sub-Section*

Great Britain one Sub-Section**)

Sub-Section b - France
Spain
Portugal
Brazil
Switzerland
) were no longer worked on. Volume of traffic was always extremely small and thus unimportant.
Head:- Oberinspektor Otto Kuehn***
(previously Sonderfuehrer (Z) Hans-Wolfgang Kuehn - from 1941-Feb.1945)
Deputy:- Wachtmeister Max Horniokel

Sub-Section c - Balkan Countries
Head:- Oberleutnant Kneschke
(previously Sonderfuehrer (Z) Geisler
previously O.Reg.Rat Bailovic)
Deputy:- Wachtmeister Esterhatzio
(name might be spelt Esterházy)

---

* Head:- Regierungsbaurat Steinberg (transferred to H.Q. Chi/OKW)
Deputy:- Unteroffizier Lucius

** Head:- Oberinspektor Zillmann (later in another Section of Gen.d.N.A.)
Deputy:- Dr. Schulz

*** Oberinspektor Otto Kuehn was previously in charge of the Main Section "Training". Associated with this were the examination, selection, and training of cryptanalysts. From the middle of March 1945, the training section was incorporated in the French Section. Before and at the beginning of the war, Oberinspektor Otto Kuehn was in charge of the French Section.

Main Section 3 Cryptanalysis "East" - Russian, to some extent Poland

Head:- Leutnant Dettmann
(before him Oberleutnant Schubert
before him Sonderfuehrer (K) Bleschke)

a) N.K.V.D. traffics (?) Leutnant Dettmann

b) Inspektor Torunsky

c) Wachtmeister Fuchs

Main Section 4 Hollerith Section and workshops

Head:- Regierungsbaurat Schenke

The main depot was at Erfurt
There was a sub-depot at Weimar

I do not know whether there was still a possibility of a change of location and whether such a move was actually carried out at the beginning of April 1945.

I/C Workshop:- Inspektor Schuessler
(Erfurt)

Main Section (Z) Personnel Matters

Head:- Inspektor Strahlendorff

Under the command of Gen.d.N.A. were the Sigint Commanders*

In service in the East (as far as I know) were:- Commander 1
Commander 2
Commander 3

In service in the West were:-

Commander 6 in the northern part of the western front

Unit Commander:- Major Lechner
I/C Cryptanalysis:- Leutnant von Demfer

---

* Very recently (exact date unknown) the following were set up:-

Senior Commander Sigint East

O.C.:- Unknown

and Senior Commander Sigint West

O.C.:- Oberst Kopp or Knop (or similar name)

I do not know whether this new organisation came into full use. This reorganisation was not supposed to make any difference to the direct contact between the head of Section 4 (Cryptanalysis) and the officers i/c Cryptanalysis of the Commanders.

Commander 5 in the southern part of the western front

Unit Commander:- Major Marquard
I/C Cryptanalysis:- Oberleutnant Schlemmer

Commander 7 - Italian front

Unit Commander:- Oberstleutnant Seemueller
I/C Cryptanalysis:- Hauptmann Mueller

From January 1941 on, the actual date of establishment of the Cryptanalysis Section, the Section was under OKH/In 7. It was not put under the command of Gen.d.N.A. till February 1945.

Heads of the Section were:-

Major Mang

Major Mettig

Major Lechner

Major Dr. Hentze

As far as I know, there was in the army before the war only a cryptanalytic section for France, Russia and Poland. All other departments were only created during the war. Army cipher systems are said to have been handled by OKW/Chi.

FRENCH CIPHER SYSTEMS (ARMY)

French Machines

1. French "C 36" Machine. This machine was worked on and frequently broken in Wm. Doering's machine section. As far as I know and can judge, the content was moderate to good, but mostly too old.

2. French "B 211" Machine. This machine was worked on in Wm. Doering's machine section without the slightest success. This machine was pronounced unbreakable by Doering and his colleagues.

3. French "BC 38" Machine. This machine was worked on in Wm. Doering's machine section. According to reports, only messages with the same or nearly the same indicator group were breakable. Under favourable circumstances the appropriate day's traffic could be broken from this. Such compromises were very rare. They were of no particular importance as the messages broken were too old.

DUMEY SAYS THIS REFERS TO THE M-209 (Ed.)

French Cipher Systems Previously Used

4. 5/L Systems. Simple transposition
10-daily key-change
appeared about June, July, August, 1943 in Tunisia.
Content insignificant

5. 3/L System. Code table.
Fortnightly key-change
Appeared from about 1942 to middle of 1944 in Syria - not intercepted after this.
Content - as far as I know and am capable of judging - moderate to good.

6. 3/L System. Code table
Fortnightly key-change
Appeared roughly 1943 to middle of 1944 - not intercepted after that - Syria.
Same system as that mentioned in para. 5.
Content - technical details of wireless traffic. Sometimes it passed the weekly changing call-signs.

7. In Syria there were also used a number of quite simple systems of rare occurrence
a) a frequently changing 2/F substitution table (with alternative equivalents)
b) a simple transposition
Content - police matters

8. 4/F System. 4/F code table
Daily key-change, but the same each month (?)
Appeared 1944 in the Syrian coastal network
Content - ship movements in coastal area.

Current French Systems

9. 5/L Messages. Diagonal transpositions.
Formerly a monthly - lately a fortnightly key-change
1943(?) - 1944 - 1945
West Africa
As far as content was concerned, only the strength returns were important.

10. TTSF. 4/L Messages. 4/F code deciphered by means of a letter substitution table
1944 - 1945
France (?) and North Africa
Content - traffic-routine messages

11. 5/L Messages. Diagonal transposition
1943 - 1944 - 1945(?)
Equatorial Africa
Content - little importance

12. 5/F Messages. 4/F code - hatted
A.T.M.43
1943 - 1944 - 1945
North Africa - Corsica
Content - good [at that time it concerned troop movements - to North Africa (coming from West Africa)]

13. 4/F Messages. 4/F code with subtractor
1944 - 1945
for a short time - Italian front
later - Mother country

14. 3/F Messages. 4/F code with subtractor
1944 - (1945 very slight, unimportant and irregular traffic) - transport network - North Africa.

A System Still Used but Unbroken when I left OKH

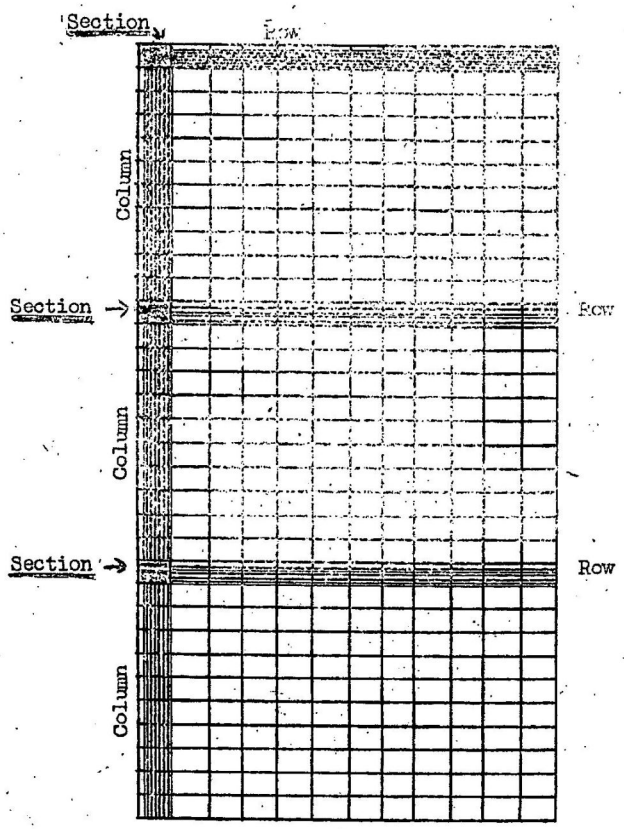
15. 5/F Messages
1943(?) - 1944 - 1945
France - North Africa - West Africa - Equatorial Africa

Description of French Cipher Systems with Details of Experience acquired in Breaking them

The French machine systems (cf. page 6 under Nos. 1 to 3) were without exception handled in the machine section under Wachtmeister Doering. I am therefore unable to give more exact details of working methods. Doering's colleagues were very carefully selected brains, men who were engineers or mathematicians in civil life.

The system mentioned on page 6, under No. 4, came up suddenly - had only a short period of validity - was of little content value - was little used. We can easily dispense with a description of the breaking process. You get the clear text by sliding ((sections of)) the cipher text against one another, later called just "sliding" for short.

The system mentioned on page 6, under No. 5, is a small 3/L code table, composed of several parts.



The construction of the code-table could be represented as shown in the diagram.

The individual code equivalent is read off in the following order:- column, section, row.

The strips (columns and rows) do not contain the whole alphabet.

The code table is arranged alphabetically. The numbers are in their natural order in the code. The recovery of the code presented no great difficulty - as stereotyped beginnings came up very often, these being addresses with name of station and location. In these, place names were usually spelt out, which made the recovery of the code still easier.

Example of a stereotyped message beginning:-

TELE - K - A - ME - CH - LI - E - A - TELE - A - LE - P - STOP

or TELE - A - LE - P - A - TELE - DA - MA - S

and similar beginnings.

Later, code recovery would have come up against considerably greater difficulties as the French introduced frequently changing 3/L cover groups for the names of stations and the most important place-names.

The key-changes carried out might be pictured as pasting new strips over the old ones.

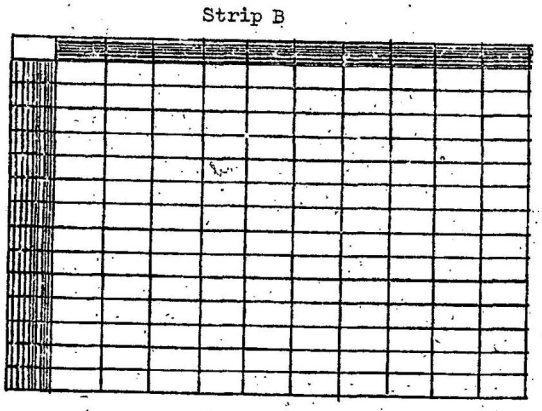
The system described on page 6, under No. 6, is a traffic-routine code identical in its entire construction to the system mentioned under No. 5. The vocabulary is more adapted to wireless traffic.

For simplicity's sake I can dispense with any further notes on the system described on page 6, under No. 7.

The cipher system quoted on page 6, under No. 8, was not broken in OKH but by Oblt. Kneschke, at that time with Sigint-Commander 4 in Belgrade. I cannot therefore give exact details without special data.

Strip B

Strip A



Each compartment of Strips A and B contains a two-digit number. So for each code item there is produced a 4-digit number. The 4/F code equivalent was further reciphered by means of figure substitution tables.

If my memory continues to serve me correctly, the figure-substitution tables changed daily, although in a monthly cycle.

The system mentioned on page 7, under No. 9, is a diagonal transposition such as must have appeared in the first world war, according to a captured description, and appeared at the beginning of the second world war in the campaign in the west.

In the two cases just mentioned this diagonal transposition had the following characteristics. In front of the cipher groups the following figure groups (for example) occurred:

[1] 00027 [2] 23322 [3] 34043 [4] 12525

[1] is the message number

[2] is the indicator group

A - B - item giving the key word

C being a repeat of B

D & E appear only as 00 or 22 or 44

Here "00" indicates no shortening of the keyword. "22" means shorten the keyword by one letter at the beginning and one at the end.

"44" shorten the keyword by 2 letters at the beginning and 2 at the end.

[3] the starting point for diagonals

[4] number of elements

Example of Encipherment

Clear text:- IN EINER FRUEHEREN SPORTHALLE IN KARLSRUHE SIND UEBER HUNDERT VERHAFTETE UNTERGEBRACHT STOP

Let the keyword be:- Paul Ambroise Valery - 10-23-37-45-73-

The numerical key is:- 12 1 16 8 2 10 4 13 11 7 15 5 17 3 9 6 14 18

Then the clear text is put in

4	11	8	18	12	2	14	5	3	17	7	15	9	13	1	16	6	10
P	A	U	L	A	M	B	R	O	I	S	E	V	A	L	E	R	Y
12	1	16	8	2	10	4	13	11	7	15	5	17	3	9	6	14	18
I	N	E	I	N	E	R	F	R	U	E	H	E	R	E	N	S	P
O	R	T	H	A	L	L	E	I	N	K	A	R	L	S	R	U	H
E	S	I	N	D	U	E	B	E	R	H	U	N	D	E	R	T	V
E	R	H	A	F	T	E	T	E	U	N	T	E	R	G	E	B	R
A	C	H	T	S	T	O	P										

Instructions for reading off diagonals

→ Instructions for reading off verticals

5 diagonals are used.

Let the starting point for the first diagonal be "3". Here the even number diagonals go to the right and the odd number diagonals to the left. The remaining letters are read off vertically beginning immediately to the right of the starting point of the diagonals (see the example).

Starting point of the first diagonals

Starting point after the diagonals have been read off

The cipher text for the above example with the appropriate indicator groups would run as follows:-

00027	23300	34043	80080		RRUVR
EEUHK	REPNU	VUIBE	TESEG	ELUTR	IOEEA
FTSTB	EHETI	HHENE	PHRNR	SRONA	DFSLD
RLEOA	TRREN	IHNAT			

Decipherment follows the same course, but in reverse.

To complicate further the diagonal transposition appearing in West Africa, the French introduced letter substitution tables with a monthly change for the numerical indicator groups. The indicator groups thus transformed were distributed, when they changed each month, the cipher text.

Suppose the letter substitution table to be:-

0	A, M, W
1	F, P, Y
2	D, R, Z
3	L, O, V
4	K, U
5	B, Q, S
6	H, X
7	E, G
8	J, N
9	C, I, T

After recipherment by the letter substitution table the indicator groups used in the above example would run:-

AAWZG RLOWM VUAKL JAINM

If now several messages are compared with one another, the indicator groups stand out if there is enough material for comparison. This was, of course, only possible by the use of statistical methods. For this purpose the first ten and the last five groups were studied statistically.

Then all first, second etc. groups of the whole material were compared, so that the indicator groups could be recognised. Owing to the characteristic construction of the indicator groups the appropriate substitution table can easily be broken.

An example of a deciphering process will be carried out with the diagonal transposition used for Equatorial Africa. The experiences gathered in the decipherment of diagonal transposition will likewise be noted there (cf. pp. 12 and 13).

The system mentioned on page 7, under No. 10, is a 4/F code, reciphered by letter substitution tables.

The single figures of the 4/F code are transformed with the aid of the letter substitution table into a 4/L cipher text. The first group in this type of message is always "TTSF". Then follows the cipher text - the last group is an indicator group. The first and last places in this group indicate the letter substitution table to be used.

By lining up messages with the same substitution tables, identical code groups or even longish repeats can be noted. Such longish repeats will usually show small gaps - thus letters can be equated with one another.

In this way the breaking of the letter substitution table is possible.

Here, too, frequently recurring stereotyped message beginnings in the initial stages made code recovery considerably easier.

Such stereotyped message beginnings were:-

Suite votre numéro ..... (numbers)
Suite votre no. ..... (numbers)
Référence notre no. ..... (numbers)
Référence votre télégramme numéro .....
Ref. votre ..... (numbers)
Numéro ..... (numbers)
Réponse à votre message ..... (numbers)
etc.

This "TTSF" code was alphabetically constructed. The first code equivalents were very quickly obtained from such stereotyped message beginnings. The numbers, which were in numerical order, provided further possibilities for building up the code. Lining-up of different indicator groups looked very promising from the fact that when the system was introduced nearly every message ended with the item "STOP", "FIN" or less often "POINT".

Next of all a few other items such as DE, A and some names of months were successfully identified. As far as I can judge, the content value of these messages was small.

Later such stereotyped message beginnings and endings were no longer to be seen

The diagonal transposition mentioned on page 7, under No. 11, contained chiefly official journey returns, in addition medical reports were sent in on this system.

The external characteristics of the system were:- The first two groups are 5/F groups - then follow 5/L groups, the cipher text - the last group is again a 5/F group - it is in fact identical with the second 5/F group in its first three digits.

The first 5/F group is the message number

The second 5/F group is the indicator group

The last 5/F group is a check group.

Example

00135	63798	AREEH	.....	.....	cipher text goes on .....
.....	.....	BIONE	63713		

The system was broken, but without it being possible to discover the significance of the indicator group. It could only be established that when the indicator group (i.e. the second 5/F group) was the same, the same keyword was also used.

In this system there appeared from 2 to 7 diagonals which were fixed by the indicator group. The diagonals were also read off to right and left. As far as I remember, about 600 different indicator groups appeared, of which approximately 150 were broken by my colleagues.

Work on the system just described went on for a very long time without results. Several times the work was interrupted or taken over by other cryptanalysts. Finally a lucky chance produced the solution. A message came in containing double letters in its cipher text.

Example of the breaking process:-

Only the cipher text follows - the indicator groups are not taken into consideration.

IAONR	RNOTM	QUSGR	NASRX	STNTT	LOTII
ETURU	IDXEU	OODTO	ENINP	PRXEG	EEUXG
EUSSM	SESNA	RG			

		X	X	D	E				
		G	S	X	N				
		E	T	E	L				
		U	N	U	N				
		S	T	O	P				
		S	T	O	P				
		M	L	D	R				
		S	O	T	X				

On the basis of the double letters in the cipher text it was assumed that "STOP" might occur twice directly over one another. The framed part of the adjoining example might be taken as a favourable starting point. An attempt was made to carry on the letters "TEL" to form "télégramme" - the "E" in front might be "notre" or "votre". Those attempts were therefore carried out. "M" appears twice in the cipher text. The more favourable case is shown in the example.

		E	T	E	L	E	G	R	A	M	M	E
		U	N	U	N		R			S	Q	U
		S	T	O	P		N		d	E	U	X
		S	T	O	P		A			S	S	G

After many attempts the diagonal transposition box was successfully recovered

5	9	1	3	14	2	7	11	13	15	6	10	12	8	4
S	U	I	T	E	N	O	T	R	E	T	E	L	E	G
R	A	M	M	E	N	R	O	X	U	N	U	N	T	R
O	I	S	Q	U	A	T	R	E	S	T	O	P	U	N
X	D	E	U	X	R	J	E	N	S	T	O	P	R	A
S	X	S	S	G	G	I	N	G	O	L	D			

Let me add that in this example it can no longer, of course, be a case of the original text. In the original text the words ".otre télégramme", "stop" occurred twice and the expression "SSGGINGOLD" occurred also; and these were again used. In this case only two diagonals occurred.

Two or three further messages with this indicator group were available, which could thus be broken. Here, too, the ending in "SSGGINGOLD" was repeated. "Sg" means "signé" - S-G is repeated up to three times. Ingold is a name.

In the further solutions of indicator groups successful use was again made of the more or less frequent stereotyped beginnings and endings. Here very profitable use was made of messages of equal length and with the same indicator group.

The breaking of every single indicator group made great demands on the endurance and zeal of the individual, for here only the most laborious study of details offers a prospect of success.

Here let me sum up my experience in working on diagonal transposition. The first breaking of a diagonal transposition can be considered a great piece of luck. If, however, something more is got out of this solution - such as, for example, stereotyped beginnings or endings, then that is really a big step forward.

Thanks to the stereotyped passages we were able to carry out further work on the material from Equatorial Africa with a certain amount of success.

The knowledge gained of the content of material from West Africa which also inclined towards stereotyped beginnings, supplemented and simplified the analytical work here too to a not inconsiderable degree.

Nevertheless breaking takes a very long time. Whether working on diagonal transpositions from front-line traffics with, for example, a daily change of keyword, could still be called worth-while, seems to me very doubtful.

The system mentioned on page 7, under No. 12, appeared for the first time about the middle of 1943 in North Africa. By the months March-April 1944 the system had been so far broken that the first messages could be read.

A numerical count of this material was put in hand. It turned out that the number "6" took up 14-15%. From this it could be concluded that it must be a case of a hatted code.

The external characteristics of this system are as follows:-

00075 35035 08483 59514

37485 ..... cipher text continues

1st group - message number

2nd group - number of groups

3rd group - indicator group

4th group - check group

In every message it is seen that the reversed 4th group subtracted from the 3rd group always produces the same difference.

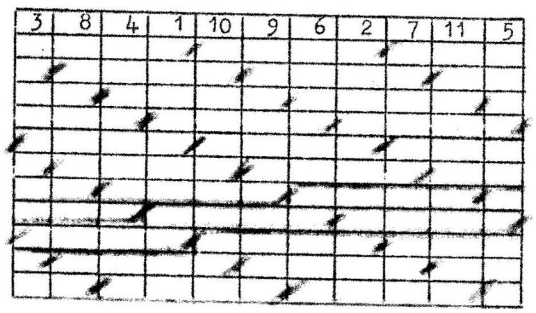
In the present case therefore:

indicator group:	08483
check group reversed:	41595
difference:	67998

In the course of time we got a number of cribs which made further work possible and assisted it, although they did not supply any particular aids for obtaining a solution.

Finally we got 5 messages with the same indicator group; all the messages were of different lengths, they all had the same contents with a further addition. The last group of each message was always identical.

The following picture resulted after the 5 messages had been arranged by "sliding".



On the basis of repetitions it was established that the foundation was a 4/F Code. The red strokes (/) show the delimitations of the individual code groups

— length of message 1
— length of message 2
— length of message 3
— length of message 4
length of message 5

By "sliding" it was then established that the last group of each message was the same (now, as was later established, meant "fin").

But this problem shall be explained more fully by means of a figure example

The cipher texts of the 5 messages run:-

Message 1:

00091 17017 08483 59514
1) 2) 3) 4) 5)
15325 11501 07734 37610 78163 03682
6) 7) 8) 9)
12826 36581 02589 15250 72765 36461
10) 11)
93121 76457 67276

Message 2:

00092 18018 08483 59514
15325 18501 07724 37610 71816 30323
82128 26636 58162 58915 65072 76553
64619 71217 64976 72763

Message 3:

00093 20020 08483 59514
15325 18950 10772 64376 10710 81630
32782 12826 36365 81662 58915 61507
27658 03646 19701 21764 91767 27635

Message 4:

00094 21021 08483 59514
15325 18935 01077 21437 61071 68163
03275 82128 26563 65816 62258 91567
50727 65813 64619 70112 17649 10767
27638

Message 5:

00095 26026 08483 59514
15325 18973 05010 77212 91437 61071
67381 63032 78278 21282 65206 36581
66546 25891 56708 55072 76581 65364
61970 31812 17649 11417 67276 38103

Repeats of message 1 in the other messages are bracketed and underlined.

Then to begin with the columns revealed by the repeats of the cipher text were written out and arranged in order of length to give the following picture:

1	2	3	4	6	7	8	9	10	5	11
1	5	4	8	6	2	5	3	1	8	7
5	0	3	1	3	5	0	6	2	2	6
3	1	7	6	6	8	7	4	1	1	7
2	0	6	3	5	9	2	6	7	2	2
5	7	1	0	8	1	7	1	6	8	7
1	7	0	3	1	5	6	9	4	2	6
1	3	7	6	0	2	5	3	5		

Message 1
So far it has thus been possible to determine that columns 5 and 11 must be the last two columns of the cage, though they might certainly be switched round → indicated by = ⌣

3	4	8	1	2	6	7	9	10	5	11
7	2	5	8	2	6	6	7	9	6	3
1	3	5								

Message 2
Columns 3, 4 and 8 must be the first three columns - but may come in a different order relative to one another.

X

3	8	4	1	2	6	7	9	10	5	11
7	5	2	8	2	6	6	7	9	6	3
1	8	7	9	6	6	1	0	1	3	5
0	0									

Message 3
Column 4 can be considered fixed. On comparing messages 2 and 3 one is struck by the figures underlined.

X

3	8	4	1	6	9	10	2	7	5	11
7	5	2	8	6	7	9	2	6	6	3
1	8	7	9	6	0	1	1	7	5	8
6	1	5	3	2	1	0				

Message 4
Further columns could thus be bracketed. Note underlining.

X X . X

3	8	4	1	6	9	10	2	7	11	5
7	5	2	8	6	7	9	2	6	3	6
1	8	7	9	6	0	1	1	7	8	5
6	1	8	7	5	3	1	2	0	1	2
7	6	2	3	4	1	4	9	8	0	0
3	5	7	0	6	8	1	1	5	3	

Message 5
It was also possible to fix columns 5 and 11. The repetition of "153" is striking.

If messages 1-5 are transcribed with the key narrowed down as far as possible, the following picture is produced:-

	3	8	4	1	6	9	10	2	7	11	5
	4	5	8	1	6	3	1	5	2	7	8
	3	0	1	5	3	6	2	0	5	6	2
	7	7	6	3	6	4	1	1	8	7	1
	6	2	3	2	5	6	7	0	9	2	2
	1	7	0	5	8	1	6	7	1	7	8
	0	6	3	1	1	9	4	7	5	6	2
↓	2	5	6	.1.	0	.3.	.5.	3	2		

Message 1

↓	7	5	2	8	6	7	9	2	6	3	6
	.1.	.5.	3								

Message 2

↓	7	5	2	8	6	7	9	2	6	3	6
	1	8	7	9	6	0	1	.6.	.1.	5	3
	0	0									

Message 3

↓	7	5	2	8	6	7	9	2	6	3	6
	1	8	7	9	6	0	1	1	7	8	5
	.6.	.1.	5	.3.	2	1	0				

Message 4

↓	7	5	2	8	6	7	9	2	6	3	6
	1	8	7	9	6	0	1	1	7	8	5
	6	1	8	7	5	3	1	2	0	1	2
	7	6	2	3	4	1	4	9	7	0	0
	3	5	7	0	.6.	8	1	.1.	.5.	3	

Message 5

If the group "6153" is assumed to be fixed, then columns 2 and 7 would have to be adjacent (message 3 - confirmation in message 5). Further columns 3 and 8 would have to be adjacent in message 4 - confirmation message 2. If message 1 is further compared with message 5, we get the following numerical key:- 3. 8. 4. 1. 10. 9. 6. 2. 7. 11. 5.

The appropriate keyword was recovered from the numerical key. I can no longer remember what it was.

An attempt was made to explain the significance of the indicator group and the check group:-

The French take the keyword from the code. The 5th digit might therefore give the starting point for the transposition.

Example:-

Suppose the code equivalent of a keyword used is 2834. Let the starting point be 1.

Then the unreciphered indicator group would read 28341.

The indicator group is reciphered by the addition of a constant five-digit number.

The check group is derived from the addition of a second five-digit number to 28341.

Example:-

*)	28341	28341 *)
	80142	23254
	08483 (indicator group)	41595 (check group reversed)

(cf. message example on page 14)

Here too, chance came to our aid. The two five-digit numbers were announced in a system we could read (C 36). Thus we had the indicator groups "in clear".

A statistical analysis of the code groups that had appeared up till then proved beyond all doubt that the code equivalent was not entered in the cage in the form "ABCD" but in the form "CDAB" (this was not carried out in the case of the example given).

The pages in the sixties were especially numerous, so the natural assumption was that the numerals and amplifying groups are to be found on these pages. This assumption was further strengthened by the fact that the statistical analysis of the decoded indicator groups showed these pages to be unused.

There were available in the way of captured documents a series of codes of similar construction. Specially notable in this connection was the "ATM" code, which must have been already in use in North Africa before the war. It was perfectly obvious that it could not be the same code. But it was possible to use the vocabulary of this code to an extraordinarily great extent. Thus the new code - it was named "ATM 43", as was discovered later from decoded messages - could be recovered with quite remarkable speed and worked on with good results.

Later the indicator group technique for this system was changed. The position of the indicator and the check group varied with the length of the message.

The position of the indicator and check groups was related to the group giving the number of groups.

Examples:-

Number of groups	Position of indicator and check group
10010	in positions 1 and 2
11011	" " 2 " 3
12012	" " 3 " 4
13013	" " 4 " 5
20020	" " 2 " 3
21021	" " 3 " 4

The first and second digits of the number of groups are added, giving the position of the indicator group - the following group is always the check group

---

*) The same difference in all messages comes from subtraction of the constants

80142
23254
67998 (cf. page 14)

The recipherment was as follows:-

28341	28341	indicator group
10091	94520	date 10. 09. 1945
38332	12861	+ 20
		30 (September - 30 days)

Solution of this recipherment took an extremely long time; success finally came by "sliding" a short message. "Sliding", also called "dragging" was looked on as a last resort and was carried out by a large staff; it finally brought success.

The system mentioned on page 7, under No. 13, is a 4/F code reciphered with a short subtractor, which was used on the Italian front in the early days and was captured there. Later the same code turned up in France too.

Example:-

0023 1717 4543 1721 ....

cipher text continues 2582

group 1 - message number

group 2 - number of groups

last group - indicator group. Digits 1 and 4 give the same number, which indicates the subtractor.

Change of subtractor took place weekly (?).

Within a key period, 10 different subtractors are therefore possible.

By the use of short subtractors, so many depths arose that the breaking of the subtractors presented no difficulties. In this system, too, we were helped (1) by current knowledge of the message text; (2) by a series of stereotype messages. This system provided nothing important by way of content.

The system mentioned on page 7, under No. 14, is a 4/F code reciphered by means of short subtractors, which was used in transport networks in North Africa. To begin with the volume of traffic was very large - and finally in the latter days fell away to only a few messages a month.

The external characteristics of the system were the same as those already described in the previous system.

It was important for the breaking of the system that these transport reports had up till then been given in plain language. The form of these reports was kept very stereotyped.

Concerning our experiences in breaking 4/F codes with subtractor recipherment it can be said that for the most part it presents no special problems to cryptanalysis. At our station when dealing with codes with subtractor recipherment we always worked with catalogues of differences which were drawn up in the form of punched cards, with the 40-50 most frequent code groups as a basis.

Up till the middle of March 1945 we had not succeeded in breaking the system mentioned on page 7, under No. 15. Solution of this material seemed to me also very unlikely.

FrB

Let me sum up in the following section the results and experiences gained so far from working on this material.

At the same time and in the same networks as the "ATM 43" had appeared, there were a few messages which did not show the characteristic difference of the "ATM 43" but a different one. In the course of time the volume of traffic increased considerably. Two or three cribs turned up, of which only one could be worked on sufficiently to allow the key-word to be recovered. It could then be deduced from this that it was a hatted 5/F code.

It was interesting to note here that an extraordinarily small number of cribs turned up; the first crib turned up after 1600 messages; quite contrary to the previous situation.

The work was stopped. Some time before the appearance of this system 5/F material had turned up in traffic between Corsica and North Africa; it consisted of only about 80 messages. No further material came in later. This material was subjected to a brief examination. These 80 messages could be worked on. It was a case of a 5/F code which had been transposed. It was a very primitive kind of transposition.

Example of a key of this type:-

10, 11, 12, 13, 14, 15, 16, 17, 1, 2, 3, 4, 5, 6, 7, 8, 9

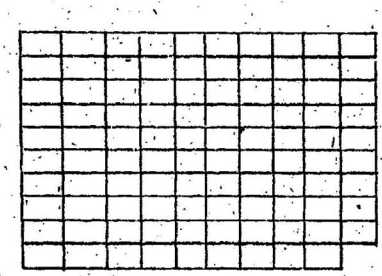
As far as I remember, the keys changed daily.

Thus these 80 messages could be worked on sufficiently to reveal the basic code groups.

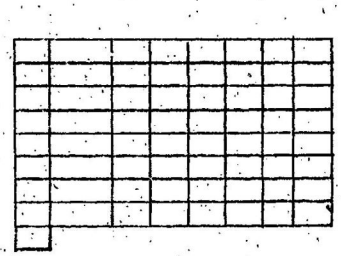
Interestingly enough it then turned out that the same code must be the basis of both systems. At this point the examination of the material with its 80 messages could be considered completed.

The material on which work had previously been suspended was taken in hand again. No new cribs had turned up. Thanks to the newly found code groups of the above-mentioned 80 messages, further study would have been highly promising. So a new approach was sought and found. Let me now describe it - I have not heard whether it did finally lead to success.

It was seen time and time again that the cage widths used in the re-cipherment must stand in some relationship to the message lengths, as it was reasonable to suppose that certain maximum and minimum depths must be prescribed for the message cages. Likewise it may be assumed that cipher regulations strictly forbid so-called "full cages". Thus we can leave out of account "sliding" of complete cages. Therefore, as one has no cribs at one's disposal, one would have to try "sliding" messages which have an overlength or underlength of 1 or 2. Such cages then would look like this:-



underlength of 1



overlength of 1

Sliding such cages is not easy, demands untiring zeal and very great powers of endurance. Here, too, a further difficulty must be borne in mind, namely that the fixing of the cage width can only be done by calculations or guess-work.

Cage widths were calculated as follows:

All messages with the same indicator group were examined to establish with what cage widths full cages would be produced - these cage widths could then be discarded. As the indicator groups occurring most frequently were taken as a starting point, it could be assumed with relatively great certainty that the cage width so obtained was correct.

These experiments were carried out on as broad a basis as possible. The messages were most carefully selected.

Unfortunately, owing to my transfer I was no longer able to see the success or failure of these experiments, so that I cannot pass judgment on this new method.

In the meantime a key change took place in this material.

Example of a message beginning:-

00012	17033	16980	.....	.....	cipher text
continues		.....	.....	71389	

Group 1 - message number

Group 2 - digits 1, 2, 3 give the message length
digits 4, 5 belong to the indicator group

Group 3)
and last (or 4th) group) - indicator groups.

(I cannot now say whether the last-mentioned group stood in 4th or last place).

The indicator groups produced the following picture:-

169807 ~~÷~~ 11)
) 15437
138933 ~~÷~~ 9)

(Whether the order was 11, then 9, or the other way round I cannot now say).

Among this material, two or three cribs had turned up, work on which had brought no corresponding results. It was assumed that this new recipherment is not only based on transposition but must also have been done on a stencil in some way. Work on this set of problems had not been started in my time.

The French "AF" code must be added as No. 16. This is a small 2/L code table, not completely filled in, which was used in front-line units. Code tables of this kind were captured. Judging from our experience up to now, various even smallish units must have different code tables. Change of tables seemed to be carried out at least once every two days.

It was once possible to break the day's traffic of a unit on 20-30 messages.

Some general remarks can be made about the French systems which I shall set down here at the end of my report to sum up my experiences.

After the campaign in the West a number of French codes were captured and worked through. If we compare all these systems with those which appeared and were broken later, we find that the Frenchman is extraordinarily conservative regarding the construction of his cipher systems or reciphering methods. Systems which must have been used in the first world war (to judge from documents found) were used during the campaign in the West and in a slightly modified form up to 1945 in West Africa.

As methods for reciphering basic books there appear principally:-

1. subtraction with finite subtractors

2. transposition, with keywords taken from the code.

The French are fond of using stereotyped message beginnings and endings; breaking was often made considerably easier by this. In describing the individual systems, these features were, of course, pointed out.

A further fundamental experience of mine is that the Frenchman has the idiosyncracy which he does not seem able to get away from, of communicating cipher matters or key changes by radio. Thus, through the diagonal system in West Africa we were able on several occasions to break the key for the C 36 machine, and once a key change for the ATM 43 code was announced, even though without giving details, in this way.

It has proved worthwhile to use Hollerith methods for large-scale statistical work - e.g. for setting up catalogues of differences, polygram statistics and the search for repeats. Statistical work on a smaller scale is more quickly done by hand.

(Signed) HANS W. KUEHN
Sonderfuehrer (Z)

(Trans. H.D.)